Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

~ World's Oldest Dot-com ~ People Are Talking! ~ Facebook Bug Bounty!
~ Epsilon Hackers Busted ~ "Killer" USB Drives! ~ Uncharted 4 Delayed!
~ Story of Yars' Revenge ~ Facebook Gender Option ~ Tails 1.3 Is Released!

~ Feds Halt Email System ~ PSN Attacked Every Day ~ Chrome Beta 42 Notes

-* NSA Sued Over Online Snooping *-
-* Microsoft Patches Old Stuxnet Flaw! *-
-* Google System Targets "Unwanted Software"! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Happy Friday the 13th - for the second time within a month! How often can you use that greeting?

Well, I have to admit that I enjoyed the one day this past week in which the temperatures were well above "normal" - in the 50's! It was beautiful, albeit short-lived. The ice dams on my roofs are finally gone; the snow in the yard has melted/packed down to around two feet (started off at 5-6 feet!); and I can actually see some patches of what is supposed to be my lawn! As long as we don't fall back into that bone-chilling cold pattern, I'll be fairly happy. And, I certainly don't want to see any more snow (let them have more in Boston if they want to break the record - just let it stay down there!).

St. Patrick's Day is coming up shortly - looking forward to an attempt to cook some corned beef and cabbage! Why not - everyone's Irish at this time of the year, so we may as well enjoy ourselves!

So, while I continue to think of my menu, I'll let you work on your appetite with another edition of A-ONE!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Sony PlayStation s Uncharted 4' Delayed!
""""""""""""""""""""""""""""""""""" PSN Attacked 'Literally Every Day'!
The Story of Yars' Revenge!
And more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Sony PlayStation s Uncharted 4’ Delayed to Spring 2016

Sony PlayStation has delayed the release of Uncharted 4: A Thief s End to spring 2016   the same year that Sony Pictures plans to release the first film based on the popular videogame franchise.

PlayStation had originally been eyeing a holiday 2015 release, but its developer Naughty Dog requested more time to finish the next installment of the Uncharted series. The third was released in 2011.

 Since we showed you our first gameplay reveal of Uncharted 4: A Thief s End, more of the game and story have come together, and it s become clear to us that this game is much more ambitious than we originally envisioned, wrote Uncharted 4? directors Bruce Straley and Neil Druckmann in a Sony PlayStation blog post on Wednesday.

The new release strategy will actually benefit PlayStation s sister company, Sony Pictures, given that the studio has dated its Uncharted film for June 10, 2016.

Moving the release date of the game by a few months was a difficult choice for Straley and Druckmann, but after spending so many years with Nathan Drake, he means a lot to the team, and telling the climactic chapter of his adventures is a task we don t take lightly   this game deserves every bit of the attention to detail, precise pacing, and nuanced storytelling Naughty Dog is known for, they added. Giving us a few extra months will make certain that Uncharted 4: A Thief s End not only meets the team s high standards but the high standards that gamers have come to expect from a Naughty Dog title.

The games biz has been looking forward to Uncharted 4, given that the title will be the first in the franchise to launch on the PlayStation 4.

The title certainly looks ambitious, with the game s graphics pushed to levels previously not seen in prior installments.

 Uncharted 4? will take place three years after Uncharted 3: Drake s Deception and force the game s hero and treasure hunter Nathan Drake out of retirement to locate a lost pirate colony.

Shuhei Yoshida: PSN Attacked ’Literally Every Day’

President of Sony’s Worldwide Studios Shuhei Yoshida recently spoke about DDoS (Distributed Denial of Service) attacks on PlayStation Network and the surprising frequency at which they occur.

At GDC this week, Yoshida told Game Informer that PSN is attacked "literally every day" and that Sony is working diligently to combat each effort.

"We are always always working against these attacks," Yoshida said. "Actually, an attack happens every day. Literally every day. Some days are bigger and some days smaller. Some days they devise new means, new ways - it’s like cat and mouse. We have a partner company we work with, and we always update the new ways the attacker might deploy, so it is a constant

battle."

Last year, on December 25, both PSN and Xbox Live were knocked offline due to large scale DDoS attacks.

Earlier this week, Head of Xbox Phil Spencer called the Christmas Day attacks a "learning experience".

Sony, Microsoft & Nintendo Are Having Conversations About DDoS Attacks

As we all remember, these past Christmas holidays brought a DDoS attack on the PlayStation Network, which made the service virtually unusable. At the same time this was going on, Xbox Live was suffering a DDoS attack, impacting their online functions as well.

At the Game Developers Conference this week, Game Informer sat down with Xbox Boss Phil Spencer, where he revealed that Microsoft, Sony, and Nintendo are having conversations and working together when it comes to protecting against these attacks:

I don t think it s great when PSN goes down. It doesn t help me. All it does is put the fear and distrust from any gamer that s out there, so I look at all of us together as this is our collective opportunity to share what we can about what we re learning and how things are growing. Those conversations happen, which I think is great.

Spencer didn t go into any further detail, only adding that the holiday downtime was a big learning experience for Microsoft.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!

The Story of Yars’ Revenge Is A Journey Back to A Lost World of Video Games

There is always a moment when the presenter will look back at the time when their particular classic game was made and say something along the lines of "crazy, crazy days."

We all know that, in the past, they do things differently. But there is one section of game-making history that is so outlandishly different from everything that came after that it takes on the quality of fantasy. The age of the Atari 2600 is a such foreign country to us, it makes later "golden eras" seem positively humdrum.

Howard Scott Warshaw’s GDC look back at his 1982 hit Yars’ Revenge offered a window into a lost world of gaming that glows for us, like a daguerreotype in moonlight.

This single-screen game of his is not some daffy adventure beloved of crusty collectors and nostalgists. Yars’Revenge, a side-ways Space Invaders-meets-Breakout with touches of Asteroids, was the most successful non-license game on the Atari 2600, a console that sold around 30 million units.

Prior to making this game, Warshaw had zero experience in game development. His main qualification was that he had "read the programming manual" for the 2600. He was motivated to work for Atari by a deep loathing of his job as a coding zombie at Hewlett-Packard.

But once he landed a job at Atari and began creating the game, he understood that a programmer could create a work of art, and enjoy the peculiar game developer thrill of watching other people enjoy that art. This was what he wanted.

Yars’ Revenge was coded with 4K bytes of ROM and 128 bytes of RAM. By way of contrast, the sound alone in 1982 arcade hit Robotron used a similar amount of memory.

Warshaw had trained as an economist. Looking back, he said, this was more valuable to him than his knowledge of programming. In an economy of scarcity, he understood how to make everything count.

Here’s an insight into just how daft those days were. Warshaw was given the task of converting arcade game Star Castle to the 2600. He thought the idea of converting that game to a console would suck, and he said so to his boss. They might just as well make a new game from scratch. Sure, the boss said, why not.

Now try to imagine that conversation going down in the meeting rooms of 2015.

It is literally made out of code

Yars’ Revenge features an insectoid space ship (Yar) ranged against an enemy ship (Qotile), encased in a defensive barricade. Yar avoids nasty missiles while shooting at, or nibbling the shield. This nibbling powers up a super weapon that can be used to destroy the Qotile, which itself powers up and attacks Yar from time-to-time.

There is an ion strip down the center of the screen. It is literally made out of code.

In its time, the game did things that were new. There was no on-screen frame to encase the action. There was no on-screen running score. The game featured an Easter egg that was part of its marketing. It was based on an elaborate back-story which included a comic-book.

This is all very interesting, especially if you enjoy those Wild West aspects of the time. But firsts were very much in the air, back in the world of 1981 video game development. You could hardly move without bumping into one.

There are a couple of stories that Warshaw shared that manage to both speak of that time, and offer lessons for today.

Firstly, he admitted that his initial run at developing the game did not go well. "The control scheme sucked," he recalled. The problem was in trying to maneuver the ship while controlling the weapon. People who

played the early builds found it irksome and difficult. But instead of trying to fix this particular problem, he changed the entire game. This was where the nibbling mechanic was born. You powered up the weapon by on-screen movement, instead of hitting a button on your controller.

The other story is more about managing hierarchies. Once an Atari game was completed, the usual form was to hand it over to the marketing team, who would weave their own particular web of magic, including giving the game a name. Then, as now, the magic of marketing wasn't very magical. "They would always end up calling the game Rock Fight or Car Drive or some two-word name like that," he said. "They all sounded stupid."

It is well known now that Yars' Revenge was named by Warshaw, that the name is an inverse of then-Atari chief Ray Kassar (Ray = Yar). Warshaw's fiction for the game includes a planet called Razak. "I always wanted to add a word to the language," said Warshaw. "I liked secret messages and hidden ideas."

I trusted that the marketing guy, when sworn to secrecy, would blab
Less well known is the story of how Warshaw managed to persuade Atari's marketing team to agree to use a name like Yars' Revenge. The truth is, he tricked them. The story illuminates the weirdness of the time, while offering inspiration to those creators at the mercy of marketing goons.

Warshaw told one of the marketing guys he wanted to pitch this name, 'Yars' Revenge.' The marketing dude was like, "OK sure, I'll talk to the team." Warshaw knew it wouldn't fly, so he said to the marketing dude, "It's based on Ray's name, but you must keep this a secret as I would not want to influence the decision." Warshaw did not mention that Ray Kassar had no notion of this game name. It was enough that the marketing guy thought Ray had sanctioned the idea.

"I trusted that the marketing guy, when sworn to secrecy, would blab," said Warshaw. Sure enough, the marketing team decided that "Yars' Revenge" would be a splendid name. Only later did Kassar find out.

After Yars' Revenge came out, and was a hit, Warshaw became Atari's feted developer. He worked on the important Raiders of the Lost Ark game, and did a good job. He met with Steven Spielberg. (All this is recounted in the excellent documentary Atari: Game Over.)

Warshaw then wanted to work on a sequel to Yars, but Atari had other ideas. They needed him to knock out a game for the holidays. That game was E.T.

During his presentation, Warshaw made a few jokes about E.T. but there was one moment when he asked the audience how many had actually played the game. A lot of hands went up. (Rare is the game developer who can count on a room full of people having played his or her game, 30-odd years after its release.)

He then asked the audience how many thought it was the worst game they had ever played. Not one hand was raised.

Warshaw's reputation as an important game developer has been somewhat resurrected by last year's E.T. dig and by Atari: Game Over. He now works as a successful psychotherapist in Silicon Valley. But I wondered how it had been for him, all these years, having made one of the most successful games ever, a model of innovation and creativity, and yet to be remembered for a game, rushed out by commercial folly? After the

presentation, I asked him this question.

"The truth is, I never saw it as such a horrible game," he said. "But I never argued with people who did. They are entitled to their opinion. I will say this, though ... I always saw games as a broadcast medium. To me, the point of media is to generate social discourse in whatever direction. The idea that 30 years later we are still talking about it... well, that feels like a great success to me. How many other 2600 games are still in the media spotlight?"

It is good that games like Yars' Revenge are being talked about, as well as games like E.T.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

US Lawsuit Challenges Legality of NSA Online Snooping

A lawsuit filed Tuesday by the operator of Wikipedia and other organizations challenges the US government's mass online surveillance programs, claiming that tapping into the Internet "backbone" is illegal.

The lawsuit was filed in Maryland federal court by the Wikimedia Foundation, Amnesty International USA, Human Rights Watch and other organizations.

It said the effort by the National Security Agency and other intelligence services "exceeds the scope of the authority that Congress provided" and violates US constitutional guarantees.

"We're filing suit today on behalf of our readers and editors everywhere," said Jimmy Wales, founder of Wikipedia, in a statement.

"Surveillance erodes the original promise of the Internet: an open space for collaboration and experimentation, and a place free from fear."

The lawsuit claims that by tapping into the Internet backbone, "the NSA is seizing Americans' communications en masse while they are in transit, and it is searching the contents of substantially all international text-based communications," effectively sweeping up data of many people unrelated to the effort to thwart terrorism.

"Rather than limit itself to monitoring Americans' communications with the foreign targets, the NSA is spying on everyone, trying to find out who might be talking or reading about those targets," said Patrick Toomey of the American Civil Liberties Union, which is representing the organizations.

"As a result, countless innocent people will be caught up in the NSA's massive net."

The lawsuit argues that based on documents leaked by former NSA contractor Edward Snowden, the NSA intercepts virtually all Internet communications flowing across the network of high-capacity cables, switches, and routers that make up the Internet backbone.

Also joining the suit are The National Association of Criminal Defense Lawyers, Pen American Center, Global Fund for Women, The Nation Magazine, The Rutherford Institute, and Washington Office on Latin America.

The defendants include the NSA and chief Michael Rogers, the office of the Director of National Intelligence and its chief James Clapper, and US Attorney General Eric Holder.

There was no immediate comment from US officials on the case.

A similar lawsuit was filed last year by the Electronic Frontier Foundation.

State Dept. Temporarily Halting Parts of Email System

The Department of State is temporarily crippling part of its main unclassified email system to boost security, according to a statement released Friday.

The agency is taking the action in order to rid the system of malware introduced by suspected Russian hackers, tweeted ABC digital reporter Justin Fishel shortly before 4 p.m. EDT.

But a statement released by the agency addressed the issue in more general terms.

"As a part of the Department of State’s ongoing effort to ensure the integrity of our unclassified networks against cyber attacks, the Department is implementing improvements to the security of its main unclassified network during a short, planned outage of some internet-linked systems," the statement read.

It continued, "There has been no compromise of any of the Department’s classified systems, nor of our core financial, consular and human resource systems."

Shortly after 4 p.m. EDT, Fishel tweeted that large parts of the system could remain down throughout the weekend.

Friday’s revelations come in the wake of controversy over the use of personal email accounts for work business by former U.S. Secretary of State Hillary Clinton.

Earlier this week, news reports indicated that suspected Russian hackers have threatened the integrity of the State Department’s email system for the last year.

Feds Indict Three in 2011 Epsilon Hack

U.S. federal prosecutors in Atlanta today unsealed indictments against two Vietnamese men and a Canadian citizen in connection with what s being called one of the largest reported data breaches in U.S. history. The government isn t naming the victims in this case, but all signs point to the 2011 hack of Texas-based email marketing giant Epsilon.

The government alleges the defendants made more than $2 million blasting out spam to more than one billion email addresses stolen from several email service providers (ESPs), companies that manage customer email marketing on behalf of major corporate brands. The indictments further allege that the men sent the junk missives by hijacking the email servers used by these ESPs.

This case reflects the cutting-edge problems posed by today s cybercrime cases, where the hackers didn t target just a single company; they infiltrated most of the country s email distribution firms, said Acting U.S. Attorney John Horn. And the scope of the intrusion is unnerving, in that the hackers didn t stop after stealing the companies proprietary data they then hijacked the companies own distribution platforms to send out bulk emails and reaped the profits from email traffic directed to specific websites.

To be clear, prosecutors haven t specifically outed Epsilon as the victim, nor did they name any of the other email service providers (ESPs) allegedly harmed by the defendants. But a press release issued today Horn s office states that the data breach into certain ESPs was the subject of a congressional inquiry and testimony before a U.S House of Representatives subcommittee on June 2, 2011.

That date aligns with a June 2, 2011 House Energy and Commerce Committee panel on the data breaches at Sony and Epsilon. Epsilon officials could not be immediately reached for comment.

Update: Epsilon confirmed that it is among the victims in this case. See the end of this story for their full statement.

Original story:

In early April 2011, customers at dozens of Fortune 500 companies began complaining of receiving spam to email addresses they d created specifically for use with those companies. On April 2, 2011, Epsilon started notifying consumers that hackers had stolen customer email addresses and names belonging to a subset of its clients.

Those clients were ESPs that send email to customers on behalf of some the biggest firms in the world. Epsilon didn t name which ESPs were impacted, but the voluminous complaints from consumers about spam indicated that those ESPs served a broad range of major companies, including JP Morgan Chase, U.S. Bank, Barclays, Kroger, McDonalds, Walgreens, and Honda, to name but a few.

A scam web site that tried to sell copies of Adobe Reader.

As I noted in that April 2011 story, consumers had complained of received junk email with links to sites that tried to sell versions of software made by Adobe Systems Inc. Some of the sites reportedly even tried to sell copies of Adobe Reader software that Adobe gives away for free.

Sure enough, the men indicted today are accused of hacking into a major

ESP to steal more than a billion email addresses, which they allegedly used to promote knockoff versions of Adobe software (among other dubious products).

Prosecutors in Atlanta today unsealed indictments against Viet Quoc Nguyen and Giang Hoang Vu, both citizens of Vietnam who resided for a period of time in the Netherlands. The government also unsealed an indictment against David-Manuel Santos Da Silva, a Canadian citizen who was charged with conspiring with Nguyen and others to launder the proceeds of Nguyen s alleged computer hacking offenses.

The government alleges that Nguyen used various methods including targeted email phishing campaigns to trick recipients at email marketing firms into clicking links to sites which attempted to exploit browser vulnerabilities in a bid to install malicious software. For more on those targeted attacks, see my Nov. 24, 2010 story, Spear Phishing Attacks Snag E-Mail Marketers.

Nguyen s phishing campaigns allegedly delivered malware, which allowed him backdoor access to the ESP employees computer systems and enabled him to steal sensitive information, including the employees access credentials for the ESP s computer systems, the government alleged. Using stolen access credentials, Nguyen was not only able to allegedly steal confidential information by downloading the information from the ESPs computer systems to a server that he controlled in the Netherlands, but was also able to utilize the ESPs computer systems to launch spam attacks on tens of millions of stolen email addresses.

Vu allegedly assisted in the spamming. Da Silva allegedly helped launder the proceeds of the spam campaigns. Prosecutors say Da Silva ran an affiliate marketing firm called Marketbay.com, and that through that service he provided Vu and Nguyen a way to monetize their spam campaigns.

If recipients of the spam emails clicked through and paid for the products advertised in the junk email, those customers would be directed through Marketbay s affiliate links. According to the government, Da Silva knew Vu and Nguyen were using stolen email addresses and hijacked ESPs to drum up sales, which prosecutors allege generated more than $2 million for the men.

Vu was arrested by Dutch authorities in 2012 and was later extradited to the United States. He has pleaded guilty to conspiracy to commit computer fraud, and is slated to be sentenced in April 2015.

Da Silva was arrested in Ft. Lauderdale, Fla. on Feb. 12, and is expected to make his first appearance today before a federal magistrate in Atlanta. Nguyen is not in custody and remains a fugitive.

Epsilon confirms that it is among the victims of the cybercrime referenced in the Department of Justice s indictment unsealed on March 5 against three individuals for their roles in hacking email service providers throughout the United States. We are pleased with the outcome of the investigation carried out by the U. S. Secret Service and the resulting indictment by the Department of Justice, and thank them for bringing this criminal activity to prosecution. Data protection is,and always has been, the top priority at Epsilon, and businesses and law enforcement must work together to prevent this type of criminal activity.

Microsoft Patches Old Stuxnet Flaw for New Attack Vectors

The Stuxnet worm was an exploit that was used against a nuclear facility in Iran back in 2010, in part by taking advantage of a vulnerability in Windows. The vulnerability that enabled Stuxnet was identified as CVE-2010-2568, which was thought to have been patched by Microsoft in October 2010. More than four years later, Hewlett-Packard's (HP) Zero Day Initiative (ZDI) has discovered that the CVE-2010-2568 fix was not, in fact, complete and the underlying vulnerability has remained exploitable the whole time.

"CVE-2015-0096 is a vulnerability in the Microsoft Windows operating system that allows remote attackers to execute arbitrary code by having the target simply browse to a directory containing a malicious .LNK file," Brian Gorenc manager of vulnerability research for HP Security Research,"The patch for CVE-2010-2568 did not completely address the issues present in the Windows Shell, and the weaknesses left are now being resolved five years later as CVE-2015-0096."

For it's part Microsoft sees the issue in slightly different light. In an email statement Microsoft stated that:

"This is a new vulnerability that required a new security update. Microsoft released a comprehensive security fix in 2010 to address the vulnerability the Stuxnet virus exploited. As technology is always changing, so are the tactics and techniques of cybercriminals. It is an unfortunate reality of today s interconnected world that some people and organizations seek to disrupt technology and steal information for nefarious purposes. We will continue to stand guard against any attempts to exploit our products and do what is necessary to help further protect our customers."

The Top Software Exploit of 2014?
The Stuxnet XP Flaw from 2010, Reckons HP

For cyber-attackers, the old flaws are still the best, according to HP's Cyber Risk Report 2014 and it has a startling piece of evidence to back up its claim the most commonly exploited software vulnerability for last year was the infamous .lnk flaw in Windows XP made famous by Stuxnet in the distant summer of 2010.

Designated CVE-2010-2568, this on its own accounted for a third of all exploits the firm detected being used against its customers, just ahead of the even older CVE-2010-0188, a flaw in Adobe s Reader and Acrobat, responsible for 11 percent of exploits.

The rest of the top-ten list was a rag-tag of mainly Java vulnerabilities dating from 2012 and 2013 with one in Microsoft Office, CVE-2009-3129, dating back to themists of September 2009.

As for the Stuxnet flaw, its use was no accident, a legacy of old exploits criminals keep trying out of habit unlike most of the old vulnerabilities its use in attacks actually grew throughout the year.

In contrast, the most targeted of the 30 popular flaws discovered in 2014

was last February s Internet Explorer 10 remote code execution zero day, CVE-2014-0322, followed by CVE-2014-0307, also in IE. All of the other top ten discovered during the year were in Flash, Firefox, Office and Windows, meaning, HP suggests, that Java might finally be getting on top of its security problems.

Many of the biggest security risks are issues we ve known about for decades, leaving organisations unnecessarily exposed, said HP s senior VP of Enterprise Security Products, Art Gilliland.

HP didn t give absolute numbers for comparison but had calculated that 44 percent of flaws came from vulnerabilities that were between two and four years old.

We can t lose sight of defending against these known vulnerabilities by entrusting security to the next silver bullet technology; rather, organisations must employ fundamental security tactics to address known vulnerabilities and in turn, eliminate significant amounts of risk.

Overall, HP s Zero Day Initiative (ZDI) had dealt with a record number of vulnerabilities during 2014, the firm said.

According to HP, the commonest non-Windows exploit was the Android Master Key vulnerability, CVE-2013-4787, discovered in July 2013, which accounted for one percent of all samples.

Google’s Safe Browsing System Targets ’Unwanted Software’

Get ready to see more red warning signs online as Google adds ammunition to its technological artillery for targeting devious schemes lurking on websites.

The latest weapon is aimed at websites riddled with "unwanted software" a term that Google uses to describe secretly installed programs that can change a browser’s settings without a user’s permission. Those revisions can unleash a siege of aggravating ads or redirect a browser’s users to search engines or other sites that they didn’t intend to visit.

Google had already deployed the warning system to alert users of its Chrome browser that they were about to enter a site distributing unwanted software. The Mountain View, California, company just recently began to feed the security information into a broader "safe browsing" application that also works in Apple’s Safari and Mozilla’s Firefox browsers.

All told, the safe browsing application protects about 1.1 billion browser users, according to a Thursday blog post that Google Inc. timed to coincide with the 26th anniversary of the date when Tim Berners-Lee is widely credited for inventing the World Wide Web.

Microsoft’s Internet Explorer doesn’t tap into Google’s free safe browsing application. Instead, Explorer depends on a similar warning system, the SmartScreen Filter.

Google’s alerts about unwanted software build upon the warnings that the safe browsing system has already been delivering for years about sites infected with malware, programs carrying viruses and other sinister

coding, and phishing sites that try to dupe people into sharing passwords or credit card information.

Whenever a potential threat is detected by the safe browsing system, it displays a red warning sign advising a user to stay away. Google also is demoting the nettlesome sites in the rankings of its dominant Internet search engine so people are less likely to come across them in the first place. Google disclosed Thursday that the safe browsing application has been generating about 5 million warnings a day, a number likely to rise now that unwanted software is now part of the detection system.

As it is, Google says it discovers more than 50,000 malware-infected sites and more than 90,000 phishing sites per month.

The safe browsing application had gotten so effective at flagging malware and phishing that shysters are increasingly creating unwanted software in an attempt to hoodwink people, said Stephan Somogyi, Google’s product manager of safe browsing.

"The folks trying to make a buck off people are having to come up with new stuff and that puts us in a position where we have to innovate to keep pace with these guys," Somogyi said in an interview. "You are now going to see a crescendo in our enforcement on sites that meet our standard of having unwanted software."

Facebook Employees Can Access Your Account Without Password

Do you know that your Facebook account can be accessed by Facebook engineers and that too without entering your account credentials? Recent details provided by the social network giant show who can access your Facebook account and when.

No doubt, Facebook and other big tech companies including Google, Apple and Yahoo! are trying to keep their data out of reach from law enforcement and spies agencies by adopting encrypted communication and end-to-end encryption solutions in near future, but right now they have access to your personal data, and at least few of their employees can access it with one click.

Earlier this week, director at the record label Anjunabeats, Paavo Siljamäki, brought attention to this issue by posting a very interesting story on his Facebook wall. During his visit to Facebook office in LA, a Facebook engineer logged into his Facebook account after his permission, but the strange part they did it without asking him for the password.

Facebook even didn t notify Siljamäki that someone else accessed his private Facebook profile, as the company does when your Facebook account is accessed from any new device or from a different Geo-location.

Siljamäki got in contact with Facebook in order to know how many of Facebook’s staff have this kind of ’master’ access to anyone’s Facebook account and when exactly they can access users private data, and also, how would anyone know if his/her Facebook account has been accessed.

When the social network giant asked about how the employee got access to user s Facebook account without entering the account credentials, Facebook issued the following statement:

"We have rigorous administrative, physical, and technical controls in place to restrict employee access to user data. Our controls have been evaluated by independent third parties and confirmed multiple times by the Irish Data Protection Commissioner s Office as part of their audit of our practices."

The company didn t explain exactly who can access what, but it assured its users that the accounts access is tiered and limited to specific job function. The access to accounts are granted to most employees in order to reply to a customer request for information or error report.

"Designated employees may only access the amount of information that s necessary to carry out their job responsibilities, such as responding to bug reports or account support inquiries," Facebook goes on explaining. "We have a zero tolerance approach to abuse, and improper behavior results in termination."

In short, the social network giant has a customer service tool that can grant Facebook employees access to a user s account. Facebook runs two separate monitoring systems that generate weekly reports on suspicious behavior which are then reviewed and analyses by two independent security teams, specifically a selected group of employees.

Facebook gives a strict warning when hired employees to use this tool and fired any employee directly who abuse it. So, you need not to worry about Mark Zuckerberg accessing your account, unless you yourself ask Facebook for help with something and have given permission.

Panda Antivirus Labels Itself As Malware, Then Borks Everything

Panda users had a bad hair day on Wednesday, after the Spanish security software firm released an update that classified components of its own technology as malign.

As a result, enterprise PCs running the antivirus software tied themselves in something of a knot, leaving some systems either unstable or unable to access the internet. A Panda spokesman confirmed the problem while advising that the issue was well in hand.

"A bad update was published temporarily today [Wednesday] that resulted in some system files being detected by the Panda engine, a replacement update was promptly published removing the error and restoring the wrongly quarantined files," a Panda representative told El Reg.

"At present we recommend NOT rebooting systems. This will allow us to update the system with the amended update. This update will also restore files previously detected," he added.

An official advisory on the problem says that the issue was limited to Panda Cloud Office Protection, Retail 2015 products and Panda Free AV. Users are strongly advised not to restart their computer until a fix is available.

El Reg heard about the Panda slip-up via a tip from reader Austin, who ought to be excused claiming overtime on the back of the problem.

"Dozens of installs of Panda Antivirus across multiple sites all just detected components of itself as a virus, simultaneously," Austin explained. "Perhaps 60 in total across five sites, out of an installed base of around 300."

"If you let it disinfect ’the problem’ with a reboot, you have no network access post-reboot."

"Files we’ve seen ’detected’ include psanmodrep.dll and alertsmanager.dll both key components of Panda Antivirus itself," he added.

Users of Panda’s antivirus took to Twitter to air their woes.

False positives involving antivirus updates have affected all vendors from time to time.

The consequent problems are at their worst when Windows operating system files are falsely classified as potentially malign and quarantined, resulting in unusable Windows systems. Panda’s auto-immune screw-up would have caused comparable problems.

BBC Gives Children Mini-computers in Make It Digital Scheme

The BBC will be giving away mini-computers to 11-year-olds across the country as part of its push to make the UK more digital.

One million Micro Bits - a stripped-down computer similar to a Raspberry Pi - will be given to all pupils starting secondary school in the autumn term.

The BBC is also launching a season of coding-based programmes and activities.

It will include a new drama based on Grand Theft Auto and a documentary on Bletchley Park.

The initiative is part of a wider push to increase digital skills among young people and help to fill the digital skills gap.

The UK is facing a significant skills shortage, with 1.4 million "digital professionals" estimated to be needed over the next five years.

The BBC is joining a range of organisations including Microsoft, BT, Google, Code Club, TeenTech and Young Rewired State to address the shortfall.

At the launch of the Make it Digital initiative in London, director-general Tony Hall explained why the BBC was getting involved.

One of the BBC’s 50 partners, Barclays, already runs coding sessions in its branches

"This is exactly what the BBC is all about - bringing the industry together on an unprecedented scale and making a difference to millions," he said.

"Just as we did with the BBC Micro in the 1980s, we want to inspire the

digital visionaries of the future. Only the BBC can bring partners together to attempt something this ambitious, this important to Britain’s future on the world stage."

It is hoped that the Micro Bit will encourage children to get involved in coding and programming.

The BBC Micro, launched in the 1980s, played a big role in making computing mainstream but it was not without controversy.

The broadcaster’s decision to link up with Acorn Computers angered Sir Clive Sinclair as he prepared to launch a rival machine, the ZX Spectrum.

The BBC does not see Micro Bit as a rival to similar computing devices such as Raspberry Pi, Arduino, Galileo and Kano, but rather hopes it will act as a "springboard" to these more complex machines.

The tiny programmable machine is still a prototype and the BBC is working with several partners, including chip-designer Arm, Microsoft and Samsung, to get the end product right.

When it launches in September it will be compatible with three coding languages - Touch Develop, Python and C++.

The device is tiny - fitting easily into the palm of a hand. Children will be able to create text via a series of LED lights and they will also be able to use it to create basic games.

The final version will have a Bluetooth link enabling it to be hooked up to other devices such as a Raspberry Pi.

The Raspberry Pi Foundation is helping to develop learning resources for it and the BBC is being careful not to repeat the mistakes of the BBC Microcomputer launch, which angered rivals such as Sinclair.

BBC Learning’s Gareth Stockdale, who is developing the device, said: "The BBC’s role is to bring focus to the issue, and then we will withdraw from the market."

After the first million Micro Bits go out to schools, there will be no more.

One day they might become a museum piece like the BBC Micro, which is now housed at the National Museum of Computing at Bletchley.

As part of its Make it Digital programme, the BBC has also launched an apprenticeship scheme for 5,000 young unemployed people to boost their digital skills.

The scheme is the first of its kind to be developed in partnership with the Department for Work and Pensions.

Radio 1, which is closely involved in the initiative, will offer top-performing trainees the opportunity to go on to an apprenticeship at the station.

The nine-week traineeship, which will include training from the BBC Academy, aims to teach basic digital skills such as creating websites and short videos for the web.

The BBC is also drawing on its vast vault of content to bring digital content into shows such as Doctor Who, EastEnders and the One Show. Radio 4 will have a series of programmes that look at the history of coding, digital content and future technologies.

"With a dedicated season of programming on the BBC, 5,000 digital trainees, one million children who take their first steps with a Micro Bit, and a host of educational activity, we hope to inspire a new generation to get creative with digital," said Jessica Cecil, controller of Make it Digital.

Tails 1.3 Released

Tails 1.3 has been released.

Tails is a live system that aims to preserve your privacy and anonymity. It helps you to use the Internet anonymously and circumvent censorship almost anywhere you go and on any computer but leaving no trace unless you ask it to explicitly.

It is a complete operating system designed to be used from a DVD, USB stick, or SD card independently of the computer’s original operating system. It is Free Software and based on Debian GNU/Linux.

https://tails.boum.org/news/version_1.3/index.en.html

Chrome Beta 42 Adds Website Push Motifications, Banners for Saving Web Apps to Android Home Screens

Google released Chrome 42 this week through its beta channel for Android, Windows, Mac, Linux and Chrome OS. The latest Chrome beta previews a couple of interesting features that make web apps more like native apps including push notifications and saving web apps to your Android home screen faster

Chrome 42 Beta allows web developers to support push notifications to users through Google s web browser. Similar to Safari on OS X, push notifications on Chrome require explicit user permission before being turned on. But unlike Safari push notifications, Chrome will present a somewhat unattractive but highly useful site settings link right on each notification banner to allow users to easily opt out of future alerts without having to actually find the correct settings menu to opt out.

After the user has granted permission, a developer can use the new Push API to remotely wake up their service worker using Google Cloud Messaging. Once awake, the service worker may run JavaScript for a short period but in this release it is required at minimum to show a user-visible notification.

Specifically on the Android side, web developers can now promote their high quality web apps to frequent site visitors with a new add to home screen button. The banner will appear on the bottom of the web site and allow users to save sites that meet eligibility criteria that ensure

that users have a good experience when launching sites from the home screen, even when offline.

Aside from push notifications and better web app saving, Chrome 42 Beta includes under-the-hood changes for developers as well. You can read more about the latest version on the official Chromium blog.

Facebook Adds New Gender Option for Users: Fill in the Blank

Facebook users who don’t fit any of the 58 gender identity options offered by the social media giant are now being given a rather big 59th option: fill in the blank.

"Now, if you do not identify with the pre-populated list of gender identities, you are able to add your own," said a Facebook announcement published online Thursday morning and shared in advance with The Associated Press.

Facebook software engineer Ari Chivukula, who identifies as transgender and was part of the team that made the free-form option, thinks the change will lead to more widespread acceptance of people who don’t identify themselves as a man or woman.

"We’re hoping this will open up the dialogue," Chivukula said.

Alison C.K. Fogarty, a gender identity researcher at Stanford University, said giving users control over the words describing their gender is a significant step in social recognition of a growing trans community, especially coming from the world’s largest social media company.

"People are still fighting to make room for gender identity within the socially constructed binary of male and female," Fogarty said. "Labels and identities are powerful in that they give a sense of community, a way of articulating one’s experience."

In February 2014, Facebook expanded gender identity from male and female to a list of dozens of options, including Androgyne, Gender Fluid, Intersex, Neither and Transgender. Those choices will all still be available.

People who choose a custom gender can also choose the pronoun they would like to be referred to publicly: he/his, she/her or they/their.

Facebook has a setting for users to control the audience who sees their gender.

Last year’s changes created an online stir, with thousands of comments some grateful, others confused or hostile. But staff at Facebook said there was full support to take it even further this year, from CEO Mark Zuckerberg on down.

As of Thursday, the free-form option rolled out to U.S. users, while the custom gender identity option with a list of words was available in the United Kingdom, Canada, Australia, France, Spain, Italy, Germany, Argentina and Denmark.

One thing that has not changed is an "interested in" option for Facebook

users to define whom they might want to date. That option still only allows men or women, but users can click both options, one option or neither option. They can also hide it entirely.

Facebook, which has 1.23 billion active monthly users around the world, would not release how many users have chosen gender identity options beyond man or woman, citing privacy concerns and a general practice of not sharing user information.

The Williams Institute, a think tank based at the University of California, Los Angeles, estimates there are at least 700,000 people in the U.S. who identify as transgender, an umbrella term that includes people who live as a gender different from the one assigned to them at birth.

Sarah Kate Ellis, CEO and president of the advocacy group GLAAD, said that the past few years have brought "real movement in trans visibility" and that Facebook has been a leader in making that happen.

"This helps to accelerate trans acceptance in our country," Ellis said. "I'm excited about the future for gender identity."

Facebook Bug Bounty Report for 2014: $1.3 Million Paid Out to More Than 700 Bug Finders

We first wrote about Facebook bug bounties a shade under four years ago.

As we pointed out back then, early detractors of Facebook's bounty program were quick to call it cheap, because the bottom-level payout was $500, as it still is today.

To be fair to Facebook, that's the smallest payout you can get.

Apart from zero, of course, if you report a bug that doesn't count or isn't new.

Other companies with bug bounties actually have similar minima.

(Yahoo! famously paid out just $12.50 in company store credit to its first bug bounty winner although the company that found the bug was actually conducting its own research to see how quickly Yahoo! would react, rather than doing it for the payout.)

At the other end of the scale, the limit on Facebook's maximum payout is pretty generous: there isn't one.

So you can do quite nicely out of a reponsible vulnerablity report, as Facebook's recently-released 2014 Bounty Statistics reveal.

The company paid out a total of $1,300,000 in 2014, which is actually slightly down from 2013's total of $1.5M.

The average payout (we're assuming this is a mean average) was $1788, meaning that just over 700 people submitted bugs that were new, relevant and responsibly disclosed.

Interestingly, that means most bug submitters came away empty handed,

because Facebook reported a grand total of 17,011 reports.

Of course, that’s one of the downsides of a bug bounty programme: the need to sort the 96% of bug chaff from the 4% of exploitable wheat.

For that reason, we recommend taking a careful look at what does and doesn’t count for any bug bounty programme in which you are thinking of participating.

Facebook, for example, has published a handy list of "These Do Not Qualify" examples to help you avoid disappointment.

Notably, Facebook will not pay out on bug reports of security issues in third-party apps:

These apps are not written or managed by Facebook. We cannot authorize security testing against them and we cannot reward you for any findings.

You could earn a lot more than that $1788 average, though.

A good bet for pulling in ten times as much seem to be finding a way to delete other people’s photographs.

Facebook has paid out $12,500 on at least two separate occasions, for two different sorts of bug that could lead to unexpectedly vanishing images.

As for just how high Facebook’s unbounded-above payouts went in 2014: we don’t know.

But we can guess, because the company did note that the Big Five bug reports pulled in a total of $256,750, for a mean of just over fifty large ones each.

Another thing we don’t know is whether you can qualify for a payout by finding a bug in the "don’t bother to report these bugs" guidelines.

We spotted one, but we’re not ready to risk the embarrassment of being turned down for pedantry by reporting it. (You are welcome to try yourself, but leave a note in the comments if you do, so everyone else knows not to bother.)

Facebook explicitly warns you not to report as a bug the fact that you can enter your password with [Caps Lock] turned on and still get into the site.

That’s not a bug, it says, but a feature "to help overcome [one of the two] most common reasons that authentic logins are rejected."

(The other reason is wrongly typing in a capital letter at the start of your password, for example because your spelling checker decided you were beginning a sentence.)

Oh, really?

This ’Killer USB’ Can Make Your Computer Explode

Can Hackers turn a remote computer into a bomb and explode it to kill

someone, just like they do in hacker movies? Wait, wait! Before answering that, Let me tell you an interesting story about Killer USB drive:

A man walking in the subway stole a USB flash drive from the outer pocket of someone else’s bag. The pendrive had "128" written on it. After coming home, he inserted the pendrive into his laptop and instead discovering any useful data, he burnt half of his laptop down. The man then took out the USB pendrive, replaced the text "128" with "129" and put it in the outer pocket of his bag Amen!

I m sure, you would really not imagine yourself being the 130th victim of this Killer perdrive, neither I.

This above story was told to a Russian researcher, nicknamed Dark Purple, who found the concept very interesting and developed his own computer-frying USB Killer pendrive.

He is working with electronic manufacturing company from where he ordered some circuit boards from China for creating his own USB killer stick.

"When we connect it up to the USB port, an inverting DC/DC converter runs and charges capacitors to -110V," the researcher explained. "When the voltage is reached, the DC/DC is switched off. At the same time, the field transistor opens."

At last, he successfully developed a well functioning USB killer pendrive which is able to effectively destroy sensitive components of a computer when plugged-in.

"It is used to apply the -110V to signal lines of the USB interface. When the voltage on capacitors increases to -7V, the transistor closes and the DC/DC starts. The loop runs till everything possible is broken down. Those familiar with the electronics have already guessed why we use negative voltage here."

It is not possible for hardware to prevent all damage to physical systems in some scenarios. It may be possible for an attacker to exploit SCADA vulnerabilities and remove safety controls used by power plants or put it into an unstable state.

Stuxnet worm is one of the real example of such cyber attacks, which was designed to destroy centrifuges at the Nuclear facility and all this started from a USB drive.

Also in 2014, a security firm demonstrated an attack on Apple s Mac computer by overriding temperature controls, which can actually set the machine on fire.

So if we say that a computer could be converted into a bomb, then of course it s true, a hacker can probably make your computer explode as well.

Therefore, next time when you find an unknown USB flash drive, just beware before inserting it into your laptop. Because this time it will not fire up your important files or data stored on your laptop like what malwares do, instead it will fire up your Laptop.

The Internet is celebrating a big birthday next week: The world's oldest dot-com domain, symbolics.com, is turning 30 on Sunday.

The first dot-com was purchased by a Massachusetts-based computer company Symbolics on March 15, 1985 - four years before the World Wide Web even existed. (Email and the Internet pre-date the Web).

Symbolics was one of the original makers of computer workstations, and the company even got a mention in the movie "Jurassic Park." But the "Lisp" computer language that Symbolics developed eventually faded in popularity. Symbolics went belly-up and filed for bankruptcy in 1993.

The company and its symbolics.com website continue to exist today. Symbolics maintains the Lisp operating system that is still used by some companies and government agencies, albeit in a very limited way.

But in 2009, Symbolics got an unsolicited call from an entrepreneur named Aron Meystedt. He had built up a small domain name registry business called XF.com Investments, and he thought he'd take a shot in the dark by asking if symbolics.com might be up for sale.

Meystedt said his call was perfectly timed: The company was looking to raise money to continue its operations. Symbolics transferred the domain name to Meystedt (he can't share terms of the deal, since they were subject to a nondisclosure agreement), and the company moved its site (still the same since 2005) to symbolics-dks.com.

So what to do with symbolics.com? Meystedt said it had been - and continues to be - a frequent topic among friends, family and colleagues.

He quickly noticed that the site had been getting traffic without any advertising. Hundreds and sometimes thousands of people visit each day, and hundreds of thousands of clicks come into symbolics.com each year from curious Web browsers who happened to come across the fact that symbolics.com was the first dot-com.

Meystedt thought there could be a revenue opportunity there. So he turned it into a kind of Internet history archive. A cartoonish city on the homepage reveals fast facts about the Internet and Worldwide Web when you click on buildings' windows.

To make money on his purchase, he allows companies to sell ads. Though he brought in some ad sales in the past (he says he's unsure of the total amount), Meystedt has since taken a job that has put his symbolics.com hopes on the back burner.

Meystedt is now director of auctioning off domain names at Heritage Auctions. He recently auctioned off classic.com for $172,500 and NL.com for $575,000. His XF.com Investments company also owns the rights to tablets.com and copier.com.
Even though he isn't getting to work on his symbolics.com passion project, he doubts that he'll sell it. As a piece of Internet history, he says he is "very humbled" to be able to own it.

=~=~=~=